بنـك الرياض
Riyad Bank

SRD

System Requirements Document (SRD)
Project: User Authentication System Implementation

1. Requirement Mapping

Business Requirement	System Requirement(s)	Priority
BR1: Secure user data by requiring authentication.	SR1.1: Implement a secure registration process that requires a unique email and password.	High
	SR1.2: Store user credentials securely with encryption.	High
	SR1.3: Implement session management to maintain security.	Medium
BR2: Allow registered users to access personalized content and settings.	SR2.1: Develop a login mechanism using registered credentials that supports personalized content retrieval.	High
BR3: Support future features such as role-based access control.	SR3.1: Design system architecture to accommodate simple user/admin roles initially.	Medium

2. System Architecture Impact

Impacted System/Module	Change/Integration Description
User Interface (UI) Module	Implement new UI components for registration, login, logout, and profile management.
Database System	Modify schema to store encrypted user credentials and profile details.
Authentication Service	Implement authentication APIs for user registration, login, logout, and password reset.
Security Module	Integrate encryption protocols to secure user data storage and implement secure session handling.

3. Functional and Non-functional Requirements

Functional Requirements

FR1: Users should be able to register with a unique email and password.
FR2: Users should be able to log in using registered credentials.
FR3: Users should be able to reset their password via email verification.
FR4: Users should be able to log out from the system securely.
FR5: System should validate passwords for a minimum of 8 characters.
FR6: Users should be able to update their email, password, and profile info.

Non-functional Requirements

NFR1: Authentication system should respond within 2 seconds.
NFR2: User data should be stored securely with encryption.
NFR3: System should handle at least 10,000 concurrent login requests.
NFR4: Session management should maintain security without impacting performance.

4. Assumptions and Constraints

Assumptions

It is assumed that every user will have a unique email address.
The web application is deployed on a secure server infrastructure.

Constraints

The current project scope does not include two-factor authentication or social login options.
Role-based access control beyond basic user/admin functionality is not required at this stage.

5. Glossary and Diagrams (Appendix)

Glossary of Terms:

Authentication: The process of verifying the identity of a user.
Encryption: The process of encoding information to protect it from unauthorized access.
Session Management: The technique of managing a user's interaction session with the system.

Relevant Diagrams:

Use case diagrams and sequence diagrams detailing the flow of registration, login, logout, and password recovery processes.

Summary

This SRD outlines the requirements and system architecture impacts necessary to implement a robust user authentication system that meets the outlined business objectives. Considerations for future scalability, security, and usability are embedded within both the functional and non-functional requirements. This document also comprehensively maps business requirements to specific technical implementations for clear traceability.